

**IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA**

**Alexandria Division**

UNITED STATES OF AMERICA

v.

RUDOLPH MEKHAKIAN,

ARMEN SAPLEKCHIAN,

ANATOLY ZINCHENKO,

MUSHEGH MELKONYAN

*Defendants.*

JAN 25 2018

Criminal No. 1:18-MJ-38

**UNDER SEAL**

**AFFIDAVIT IN SUPPORT OF  
CRIMINAL COMPLAINTS AND ARREST WARRANTS**

I, Maurice Haughton, being duly sworn, depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been so employed since April 2009. I currently am assigned to the Financial Investigations Group within HSI's Washington, D.C. Field Office. I have received training in general law enforcement, including training in Titles 18 and 19 of the U.S. Code, and specialized training in computer crimes, credit card fraud and financial investigations. In addition, I am a graduate of the Federal Law Enforcement Training Center at Glynco, Georgia.

2. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States, including 18 U.S.C. §§ 1344 and 1349 (Bank Fraud Conspiracy).

3. The facts and information contained in this Affidavit are based on my training and experience, my personal knowledge, my involvement in this investigation, and information that has been provided to me by other law enforcement professionals. All observations not personally made by me were related to me by the individuals who made them or were conveyed to me by review of the records, documents, and other physical evidence obtained during the course of this investigation. In addition, where conversations or statements are related herein, they are related in substance and in part except where otherwise indicated. This Affidavit contains only the information necessary to support probable cause and is not intended to include each and every fact and matter observed by me or known to the government.

4. This Affidavit is submitted in support of Criminal Complaints and Arrest Warrants charging **RUDOLPH MEKHAKIAN, ARMEN SAPLEKCHIAN, ANATOLY ZINCHENKO**, and **MUSHEGH MELKONYAN** with conspiracy to commit bank fraud, in violation of 18 U.S.C. §§ 1344 and 1349. As set forth in greater detail below, based on the government's investigation, there is probable cause to believe that, within the Eastern District of Virginia and elsewhere, **MEKHAKIAN, SAPLEKCHIAN, ZINCHENKO**, and **MELKONYAN** knowingly and voluntarily joined together with each other and others and agreed to execute (or attempt to execute) a scheme and artifice to defraud financial institutions and to obtain any of the moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, a financial institution, by means of false and fraudulent pretenses, representations, and promises, and they did so by installing electronic devices at

points-of-sale located, using those devices to steal credit or debit card number (*i.e.*, payment card numbers) belonging to individuals who unwittingly used the compromised points-of-sale, and then utilizing those misappropriated payment card numbers to withdraw money from Automated Teller Machines (“ATMs”) or to make purchases at U.S. Postal Service (“USPS”) points-of-sale.

### **PROBABLE CAUSE**

#### **A. Overview of the Conspiracy Under Investigation**

5. Since in or around June 2016, agents with HSI and the Fairfax County Police Department (“FCPD”) have been investigating the use of skimming devices to misappropriate payment card numbers, such as credit and debit card numbers, at gas stations within the Eastern District of Virginia and elsewhere.

6. The term “skimming devices,” or “skimmers,” refers to computer hardware that can be installed within legitimate electronic payment mechanisms in order to misappropriate payment card information. In my training and experience, criminals engaged in skimming frequently target gas pumps because the electronic payment systems attached to gas pumps are not as well monitored as systems attached to traditional cash registers. I also know that such criminals usually attach skimmers to the electronic components of gas pumps that accept customers’ payment cards and read those cards in order to render payment for the purchased gasoline.

7. In my training and experience, skimming devices operate as follows. If a customer swipes a payment card through a skimming device, then the skimming device can electronically capture data from the card, such as the payment card number and any associated personal identification number (“PIN”). This data can be retrieved from the skimmer in a number of ways. If a skimming device is Bluetooth-enabled, then it can transmit the captured

data to a Bluetooth-enabled device, such as a laptop or cellular telephone that is located up to approximately 300 meters away. Conversely, a text-capable skimmer can transmit the captured data via text message to an electronic device capable of receiving text messages. Finally, an SD card-enabled skimmer requires retrieval of the SD card in order to recover the captured data. Based on the investigation in this case, it appears that the conspirators generally use Bluetooth-enabled and SD card-enabled skimmers.

8. Once payment card numbers are misappropriated via a skimmer, frequently the next step, in my training and experience, is to conduct "cash-outs," *i.e.*, to use the misappropriated payment cards to make unauthorized withdrawals from ATMs and conduct fraudulent purchases. In order to conduct cash-outs, criminals typically encode the stolen payment card number onto physical cards. The encoding process typically requires a computer and a magnetic strip reader with rewriting capability, and criminals have been known to re-encode the magnetic strips of calling cards, debit cards, or credit cards with misappropriated payment card numbers. The re-encoded cards are then used to make ATM withdrawals and/or to purchase money orders from the USPS. In my training and experience, USPS money orders are purchased because they work like cash and generally have higher maximum purchases than one could withdraw from an ATM (*e.g.*, the purchase limit for postal money orders is \$3,000, whereas ATM withdrawal limits are typically between \$400 and \$600).

9. I also know that the conspiracy described herein has victimized a number of financial institutions, and I know that, at the time of the criminal conduct, at least the following financial institutions were insured by the Federal Deposit Insurance Corporation: BB&T Bank; Capital One Bank; Citibank; and TD Bank.

**B. August 8, 2017 Traffic Stop Involving ZINCENKO**

10. On or about August 8, 2017, I traveled to a BB&T Bank location in Falls Church, Virginia, which is within the Eastern District of Virginia, along with FCPD officers, after receiving reports of suspicious activity at a nearby bank location. At the BB&T, the FCPD officers observed a white male at the outdoor ATM terminal. An FCPD detective, who was on scene, recognized this person as an individual who will be referred to herein as "T.K." This positive identification of T.K., who has a distinctive tattoo on his arm, was based on BB&T Bank ATM surveillance photos provided by BB&T Bank fraud investigators showing an individual resembling T.K. conducting fraudulent withdrawals from ATMs. T.K.'s identity was later determined during a vehicle stop described below.

11. The on-scene law enforcement officers observed T.K. attempt to engage in what appeared to be multiple ATM transactions with what appeared to be multiple payment cards. FCPD Law enforcement officers also observed T.K. leave the ATM, walk across the street to a parking lot, enter the passenger side of a black 2011 Lexus ES350 bearing Maryland license plate 1A98209, and engage in a brief conversation with the driver of the vehicle. A few minutes later, FCPD officers watched as the Lexus drove out of the parking lot, cross the street, and then park in the BB&T parking lot. FCPD officers then observed T.K. exit the Lexus and approach the same ATM terminal that he was at previously. T.K. appeared to conduct several more transactions at the ATM, again appearing to utilize multiple payment cards. Based on my training and experience as well as that of the officers on the scene, T.K.'s behavior was highly consistent with credit card fraud.

12. T.K. then was observed departing the ATM and re-entering the Lexus, which then drove out of the parking lot and proceeded westbound on East Broad Street / Route 7 toward

Arlington Boulevard / Route 50. Law enforcement officers proceeded to follow the Lexus. As the Lexus, which was traveling in the far left lane, neared the turn for Arlington Boulevard, the vehicle was seen crossing two lanes and then turning right onto Arlington Boulevard. This lane change constituted a traffic violation, and a law enforcement officer with FCPD and the undersigned Affiant initiated a traffic stop. This stop was justified by Lexus's illegal lane change and by the existence of probable cause to believe that T.K. was engaged in credit or debit card fraud.

13. Law enforcement officers then exited their vehicle and approached the Lexus. In the passenger seat, visible through the windows of the Lexus, there appeared to be multiple gift cards and calling cards. The back of some of these cards were visible, and it appeared someone had written four digit numbers in black ink on the back of these cards. Based on my training and experience, this is highly indicative of credit or debit card fraud for a number of reasons: (1) calling cards and pre-paid gift cards typically do not have PINs so the writing of PINs on the cards indicates that the cards were re-encoded with stolen payment card numbers; and (2) legitimate users of payment cards typically do not write the PINs associated with the cards on the cards themselves because that defeats the security purpose of the PINs. By contrast, fraudsters typically are unconcerned about security and frequently have too many cards with too many different PINs to remember.

14. Upon approaching the vehicle, an FCPD detective asked the driver, who identified himself as **ZINCHENKO**, to get out of the car. While making this contact, I noticed the individual in the passenger seat, who later was identified as T.K., open the vehicle's glovebox and reach into the glove box. Concerned that he may be reaching for a weapon, I immediately asked T.K. to get out of the car. During this interaction, I noticed what appeared to be multiple

gift cards within the glovebox, as well as large quantities of cash and what appeared to be money orders from the USPS. Again, in my training and experience, the presence of multiple gift cards is highly consistent with this fraud scheme, as are USPS money orders since, as stated above, they are frequently used to conduct cash-outs of misappropriated payment card numbers.

15. **ZINCHENKO** and T.K. then were placed under arrest by FCPD, and an inventory search of the vehicle was conducted by the arresting FCPD detective at the time of arrest according to FCPD's policy and procedures. This search revealed several more gift cards within the Lexus, as well as a GPS navigation unit attached to the dashboard that was displaying directions to another BB&T Bank branch in the area. In addition, three Apple iPhones were found during the search of the Lexus, one of which was observed sitting on the vehicle's front passenger seat (*i.e.*, where T.K. was sitting before he was removed from the vehicle) next to a pair of sunglasses and a stack of physical cards with numbers written in black ink rubber-banded together.

16. During a search of **ZINCHENKO**'s person that was conducted incident to his arrest, law enforcement recovered approximately \$9,800 in USPS money orders wrapped in toilet paper wrappers, along with a calling card with a four digit number written on it in black ink.

17. All of the gift cards and calling cards recovered during the traffic stop had four digit numbers on their back. In addition, law enforcement officers ran the physical cards recovered from the traffic stop, including the calling card found on **ZINCHENKO**, through a magnetic strip reader. According to the reader, all of the cards seized during this traffic stop were re-encoded with credit card or debit cards numbers that a bank or credit card company had issued to individuals other than **ZINCHENKO** and T.K.

18. In addition, law enforcement obtained bank records relating to the aforementioned

USPS money orders. A review of those bank records indicated that all of the USPS money order transactions had been reported as fraudulent. Moreover, the bank records indicated that the costs of the USPS money orders had been debited from particular bank accounts (none of which belonged to any of the defendants named in this Affidavit) and then credited back soon thereafter. In my training and experience, such credits are consistent with a bank reimbursing a customer for a transaction that he or she did not make.

19. Also on or about August 8, 2017, a Russian interpreter and I provided **ZINCHENKO** with his *Miranda* advice of rights, and **ZINCHENKO** stated that he understood his rights and wished to speak with law enforcement. During the ensuing interview, **ZINCHENKO** stated that: T.K. had paid for two rooms at an area hotel; that he was staying in room 134; and that the room had personal belongings therein. It should be noted that law enforcement officer found a room key in the Lexus that indicated it was associated with the Budget Inn, and law enforcement officers were advised by management at the Budget Inn that room 140 had been reserved under T.K.'s name and that room 134 had been reserved under **MELKONYAN**'s name (although the listed first name was "Musheyn" instead of "Mushegh") and with **MELKONYAN**'s driver's license.

20. Markedly, during the arrest and processing of T.K., FCPD law enforcement officers and I observed the Apple iPhone that was recovered from the front passenger seat of the Lexus where T.K. had been sitting (as discussed above) receive approximately 16 telephone calls. The face of the cellular telephone indicated that the calls were coming from an individual identified merely as "Rudik," which is similar to the first name of **MEKHAKIAN**.



**C. August 8, 2017 Searches at the Budget Inn in Falls Church, Virginia.**

21. On the same day as the vehicle stop discussed above, *i.e.*, on or about August 8, 2017, law enforcement officers travelled to the Budget Inn located on Lee Highway, in Falls Church, Virginia, within the Eastern District of Virginia, based on the information learned through the investigation discussed above. While observing the hotel, law enforcement saw an individual, who law enforcement officers later identified as **MEKHAKIAN**, and an unidentified male exit a beige Saturn parked in the rear of the hotel parking lot and enter room 140 of the hotel.

22. Law enforcement also noticed that a black GMC Yukon bearing Missouri license plate YK4E4A was parked at the hotel near room 140, which hotel management confirmed had been rented in T.K.'s name since on or about July 31, 2017.

23. While FCPD detectives sought a search warrant for rooms 134 and 140, FCPD uniform officers were charged with watching the rooms and ensuring that members of the conspiracy—including **MEHKHAKIAN**, who, as discussed above, was believed to be constantly calling T.K.'s phone during T.K.'s arrest—did not attempt to destroy evidence. Officers were concerned about the Black GMC Yukon described above because of its proximity to room 140 and its out-of-state plates, which was consistent with the conspirators' known use of rental cars. Accordingly, while the Black GMC Yukon was parked in a space near the hotel main office in front, FCPD uniformed officers approached the vehicle, which later was determined to have four occupants, and asked the driver for identification. As they approached they noticed crumpled up calling cards sitting on the left thigh of the individual in the front passenger seat (who later was identified as **MEKHAKIAN**). The driver then identified himself as **SAPLEKCHIAN** and the rear passengers were identified as **SAPLEKCHIAN**'s spouse and

infant child.

24. The onsite officers then called FCPD detectives to inform them that **SAPLEKCHIAN** was on location. The FCPD detective informed the onsite officers ATM surveillance images had captured an individual conducting fraudulent withdrawals at ATMs in the Eastern District of Virginia and the surrounding area, as described below, and that this individual appeared to be **SAPLEKCHIAN** based on known photographs of **SAPLEKCHIAN**. At this point, both **MEKHAKIAN** and **SAPLEKCHIAN** were detained and ultimately arrested by FCPD.

25. Incident to **MEKHAKIAN**'s arrest, FCPD seized, among other things, a cellular telephone and six physical cards with magnetic strips. Law enforcement subsequently determined that five of the six physical cards had been encoded with payment card numbers not belonging to the defendants identified in this Affidavit. In addition, law enforcement, pursuant to a federal search warrant issued by the U.S. District Court for the Eastern District of Virginia, reviewed the cellular telephone seized from **MEKHAKIAN** and found: (a) a photograph of July 5, 2017 flight reservations for **MELKONYAN** relating to travel from Las Vegas to Dulles International Airport, which is within the Eastern District of Virginia; (b) a video of **MELKONYAN** inside a hotel room that resembled room 134 of the Budget Inn in Falls Church, Virginia; and (c) a video appearing to depict **MEKHAKIAN** and **MELKONYAN** driving in an unknown vehicle in an unknown location in clothing similar to what they were wearing in certain ATM bank surveillance images that appear to depict them using compromised payment cards.

26. In addition, pursuant to the search warrant issued by a Fairfax County magistrate judge, law enforcement searched rooms 134 and 140 of the Budget Inn. A number of items were recovered from the rooms, including the ones set forth in the table below:

Room 134	Room 140
A black backpack containing three laptops, a payment card reader, a DVD, and a bundle of what appear to be hundreds of calling cards (a sampling of these cards were confirmed to contain payment card numbers belonging to individuals other than the defendants identified in this Affidavit);	A black laptop bag containing a device that, based on my training and experience, is believed to be a skimming device;
A paid in full, bill of sale for a Lexus ES350 AWD (VIN: JTHCE1KS4B0029005) in the name of T.K., which appears to be the same Lexus that was stopped by law enforcement officers on August 8, 2017.	Tools that appeared, based on my training and experience, to be associated with creating and installing skimming devices connectors
Approximately \$35,950 in U.S. currency (approximately \$35,925 of which was found within three pillow cases);	Four red Bluetooth antennas that, based on my training and experience, are capable of extending the range of skimming devices, such as the one found in the closet of the room in a black laptop bag
Approximately \$49,510.45 in money orders;	A plastic bag containing gift card packaging;
	Miscellaneous personal documents in T.K.'s name, including a Maryland Department of Correction Identification for T.K.

**D. Cash Outs by SAPLEKCHIAN**

27. During the course of its investigation, HSI has received records from TD Bank, Capital One, and BB&T. Among the records received to date are surveillance images from ATMs located in Fairfax and Alexandria, Virginia, which are within the Eastern District of Virginia. As detailed in the table below, the surveillance images depict an adult male

withdrawing (or attempting to withdraw) money from ATMs via physical cards encoded with misappropriated payment card numbers. I believe the person depicted in the surveillance is **SAPLEKCHIAN** because the face of the individual depicted appears to match **SAPLEKCHIAN**'s booking photographs.

<b>Approximate Date &amp; Time</b>	<b>Location of Activity</b>	<b>Withdrawal or Attempted Withdrawal</b>
July 8, 2017, at 12:12	BB&T ATM (AA70) 12220 Fairfax Town Center, Fairfax, VA 22033	\$500.00 attempted withdrawal via TD card ending in 7658.
July 10, 2017, at 12:49	BB&T ATM (AA70) 12220 Fairfax Town Center, Fairfax, VA 22033	\$500.00 attempted withdrawal via Capital One card ending in 8665.
July 10, 2017, at 13:46	BB&T ATM (AA71) 4117 Chain Bridge Road Fairfax, VA 22030	\$500.00 attempted withdrawal via Capital One card ending in 8160.
July 31, 2017, from 10:42 to 10:51	BB&T ATM (AC23) 5203 Franconia Road, Alexandria, VA 22310	\$1,440.00 withdrawal via BB&T payment card ending in 9820.

28. According to TD Bank, Capital One, and BB&T, the accounts ending in 7658, 8665, 8160, and 9820 respectively belonged to individuals who will be identified herein as S.S., S.A., J.L., and S.B. HSI has determined through its investigation that none of the aforementioned banks or any of the aforementioned individuals had authorized any of the defendants identified in this Affidavit to make the withdrawals (or attempted withdrawals) described above.

**E. Cash Outs by ZINCHENKO**

29. As described above, **ZINCHENKO** was stopped in Falls Church, Virginia, which is within the Eastern District of Virginia, in possession of one physical card encoded with payment card numbers that he was not authorized to possess or use and approximately \$9,800 in

USPS money orders. A review of bank records relating to these USPS money orders indicate that the money orders were purchased fraudulently.

30. In addition, as described above, the search of room 134 of the Budget Inn located in Falls Church, Virginia, yielded approximately 57 USPS money orders totaling approximately \$49,510. USPS agents thereafter conducted record checks on the purchased USPS money orders and discovered that 10 of the 57 money orders had been purchased with 5 payment numbers issued by Citibank. Bank records received from Citibank indicate that all 10 of these USPS money orders had been reported as fraudulent activity. The location and amount of each of these USPS money order purchase is set forth in the table below:

<b>Date</b>	<b>Location of USPS Money Order Purchase</b>	<b>Amount</b>	<b>Last Four Digits of Citibank Card Used</b>
August 4, 2017	U.S. Post Office 11110 Mall Circle Waldorf, MD 20603	\$2,904.80	9908
August 7, 2017	U.S. Post Office 3401 12th Street, NE, Washington, DC 20017	\$1,492.80	0647
August 7, 2017	U.S. Post Office 6481 Elm Street McLean, VA 22101	\$1,400.00	9016
August 7, 2017	U.S. Post Office 2211 Rhode Island Ave, NE, Washington, DC 20018	\$1,803.20	7721
August 7, 2017	US Post Office 4325 Gallatin Street, Hyattsville, MD 20781	\$792.05	8578

31. USPS agents were able to recover surveillance images from only one of the transactions listed in the table above. Specifically, USPS agents recovered surveillance of the August 7 transaction at the U.S. Post Office located at 3401 12th Street, NE, Washington, DC 20017. Depicted in that surveillance images is an adult male who appears to be T.K.

**F. Cash Outs by MEKHAKIAN**

32. During the course of its investigation, HSI has received records from Pentagon Federal Credit Union and Signal Finance Federal Credit Union Banks. Among the records received to date are surveillance images from ATMs located in Fairfax and Herndon, Virginia, which are within the Eastern District of Virginia, and Washington, D.C. As detailed in the table below, the surveillance images depict an adult male withdrawing (or attempting to withdraw) money from ATMs via physical cards encoded with misappropriated payment card numbers. I believe the person depicted in the surveillance is **MEKHAKIAN** because the face of the individual depicted appears to match **MEKHAKIAN**'s booking photographs.

<b>Approximate Date &amp; Time</b>	<b>Location of Activity</b>	<b>Withdrawal or Attempted Withdrawal</b>
June 17, 2017, at 13:47	BB&T ATM (A872) 5200 Wisconsin Avenue, Washington, DC 20015	\$500.00 withdrawal via Pentagon Federal Credit Union card ending in 2402.
Aug. 8, 2017, at 13:10	BB&T ATM (AC82) 11230 Waples Mill Road, Fairfax, VA 22030	\$503.00 withdrawal via Signal Finance Credit Union card ending in 9953.
Aug. 8, 2017, at 13:12	BB&T ATM (AC82) 11230 Waples Mill Road, Fairfax, VA 22030	\$500.00 attempted withdrawal via Signal Finance Credit Union card ending in 9708.

33. According to Pentagon Federal Credit Union and Signal Finance Federal Credit Union, the accounts ending in 2402, 9953, and 9708 respectively belonged to individuals identified herein as A.T., R.S., and H.M. HSI has determined through its investigation that none of the aforementioned banks or any of the aforementioned individuals had authorized any of the defendants identified in this Affidavit to make the withdrawals (or attempted withdrawals) described above.

34. It should be noted that surveillance images from in and around the times of the transactions identified in the table above depict an individual resembling **MELKONYAN** walking past **MEKHAKIAN** and up to the BB&T ATM moments after **MEKHAKIAN** completes the transactions. **MELKONYAN**'s transactions at this BB&T ATM and others are discussed further below.

**G. Cash Outs by MELKONYAN**

35. During the course of its investigation, HSI has received records from BB&T Bank. Among the records received to date are surveillance images from ATMs located in Fairfax and Chantilly, Virginia, which are within the Eastern District of Virginia. As detailed in the table below, the surveillance images depict an adult male attempting to withdraw money from ATMs via physical cards encoded with misappropriated payment card numbers. I believe the person depicted in the surveillance is **MELKONYAN** because the face of the individual depicted appears to match **MELKONYAN**'s booking photographs.

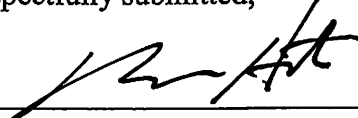
<b>Date</b>	<b>Time</b>	<b>Location of Activity</b>	<b>Withdrawal or Attempted Withdrawal</b>
Aug. 8, 2017	13:12	BB&T ATM (AC82) 11230 Waples Mill Road Fairfax, VA 22030	\$500.00 attempted withdrawal via Mid Atlantic Federal Credit Union card ending in 9953.
Aug. 8, 2017	13:41	BB&T ATM (AA70) 12220 Fairfax Town Center, Fairfax, VA 22033	\$400.00 attempted withdrawal via Mid Atlantic Federal Credit Union card ending in 3220.
Aug. 8, 2017	14:44	BB&T Bank (ATM AD13) 13360 Franklin Farms Herndon, VA 20171	\$500.00 attempted withdrawal via Mid Atlantic Federal Credit Union card ending in 0376.
Aug. 8, 2017	14:45	BB&T Bank (ATM AD13) 13360 Franklin Farms Herndon, VA 20171	\$500.00 attempted withdrawal via Mid Atlantic Federal Credit Union card ending in 2700.
Aug. 8, 2017	14:46	BB&T Bank (ATM AD13) 13360 Franklin Farms Herndon, VA 20171	\$260.00 attempted withdrawal via Mid Atlantic Federal Credit Union card ending in 9853.

36. According to BB&T Bank, the accounts ending in 9953, 3220, 0376, 2700, and 9853, respectively belonged to individuals identified herein as H.M., E.C., E.J., V.K. and G.E. HSI has determined through its investigation that none of the aforementioned banks or any of the aforementioned individuals had authorized any of the defendants identified in this Affidavit to make the attempted withdrawals described above.

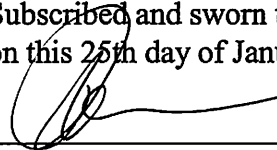
### CONCLUSION

37. In sum, based on the facts set forth in this Affidavit, I submit there is probable cause to believe that **RUDOLF MEKHAKIAN, ARMEN SAPLEKCHIAN, ANATOLY ZINCHENCKO**, and **MUSHEGH MELKONYAN** did conspire to commit bank fraud, in violation of Title 18, U.S. Code, Sections 1344 and 1349. I thus respectfully request the issuance of arrest warrants for **RUDOLF MEKHAKIAN, ARMEN SAPLEKCHIAN, ANATOLY ZINCHENCKO**, and **MUSHEGH MELKONYAN**.

Respectfully submitted,

  
\_\_\_\_\_  
Maurice Haughton, Special Agent  
Homeland Security Investigations

Subscribed and sworn to before me  
on this 25th day of January, 2018: \_\_\_\_\_ /s/

  
\_\_\_\_\_  
Theresa Carroll Buchanan  
United States Magistrate Judge

The Honorable Theresa C. Buchanan  
United States Magistrate Judge